Amendments to the Specification:

On page 6, starting at line 7, please replace the paragraph beginning "Fig. 2 is a block diagram" with the following amended paragraph:

Fig. 2 is a block diagram depicting components preferably provided at each entity in the four-corner model. As shown in Fig. 2, participants 102, 104 and root entity 110 are each preferably provided with a transaction coordinator 202 that serves as a gateway for transmitting and receiving all inter-entity messages related to services provided by the present system. Transaction coordinators 202 provide a single interface to issuing participant 102's and relying participant 104's on-line services and implement safeguards necessary to ensure secure electronic communications between transaction coordinators 202 and other entities in the four-corner model. A preferred embodiment of a transaction coordinator 202 suitable for use in the present system is described in copending United States patent application Serial No. 09/657,605, filed on even date herewith, entitled System and Method for Certificate Validation and Other Services, which is hereby incorporated by reference.

On page 6 starting at line 26, please replace the paragraph beginning "As further shown in Fig. 2" with the following amended paragraph:

As further shown in Fig. 2, relying customer 108 is preferably provided with a Web server 220 that is adapted to receive and transmit information via the Internet. Relying customer 108 is further preferably provided with a bank interface 222 for communicating with relying participant 104. One preferred embodiment of bank interface 222 (as well as additional components preferably provided at relying customer 108) is described in copending United States patent application Serial No. 09/657,604, filed on even date herewith, entitled System and Method for Facilitating Access By Sellers to Certificate-Related and Other Services, which is hereby incorporated by reference. Relying customer 108 is preferably further provided with a hardware security module 230 for signing and verifying system messages.

2

On page 7, starting at line13, please replace the paragraph beginning "The identity private key" with the following amended paragraph:

The identity private key is used to produce digital signatures that are required by root entity 110 as evidence of an entity's contractual commitment to the contents of an electronic transaction. A certificate chain is needed to support operations using this key. The status of the identity certificate may be obtained by authorized entities as described, for example, in copending United States patent application Serial No. 09/657,605, filed on even date herewith, entitled System and Method for Certificate Validation and Other Services, which is hereby incorporated be reference.

On page 7 and continuing to page 8, starting at line 26, please replace the paragraph beginning: "In a preferred embodiment" with the following amended paragraph:

In a preferred embodiment, subscribing customer 106's digital certificates and associated private keys are provided to it by issuing participant 102. Issuing participant 102 preferably issues smart cards or other suitable instruments to subscribing customer 106 that include at least the private key associated with the subscribing customer's identity certificate. If desired, the smart card may also include the subscribing customer's identity certificate. Preferred specifications for the smart card, its manufacture, and contents are described in copending United States provisional patent application Serial No. 60/224,994, filed August 14, 2000, entitled Signing Interface Requirements, Smart Card Compliance Requirements, Warranty Service, Functional Requirements, and Additional Disclosure, which is hereby incorporated by reference.

On page 9, starting at line 6, please replace the paragraph beginning "One potential implementation" with the following amended paragraph:

One potential implementation is to load an HTML page into browser 224 from a seller-side server containing the results of the negotiation of terms and conditions between buyer 106 and seller 108. Using a signed JAVA applet as part of the downloaded HTML page the information can be structured and digitally signed using smart card 226. The resulting message

3

can then be forwarded to the server for further processing. An alternative implementation approach is the use of plug-ins or helper applications, which compose and sign the payment service messages. Preferred embodiments for these implementations are described in copending United States provisional patent application Serial No. 60/224,994, filed August 14, 2000, entitled Signing Interface Requirements, Smart Card Compliance Requirements, Warranty Service, Functional Requirements, and Additional Disclosure, which is hereby incorporated by reference.

On page 9, starting at line 20, please replace the paragraph beginning "Typically, the seller uses" with the following amended paragraph:

Typically, the seller uses a standard HTTP web server (e.g., Apache) to serve HTML pages and runs an application server to provide specific business functionality to buyers, (e.g., a shopping system). Integrated with this application are other software components that facilitate access to system services including the validation and warranty services described, for example, in copending United States patent application Serial No. 09/657,605, filed on even date herewith, entitled System and Method for Certificate Validation and Other Services, which is hereby incorporated by reference, and the payment services described herein. In a preferred embodiment, this integration may be the active integration described in copending United States patent application Serial No. 09/657,604, filed on even date herewith, entitled System and Method for Facilitating Access By Sellers to Certificate-Related and Other Services, which is incorporated by reference. A seller 108's decision about payment instruments to offer buyer 106 and the resulting terms of a purchase are an integral part of the seller's application.

On page 10, starting at line 11, please replace the paragraph beginning "Applications running at seller 108" with the following amended paragraph:

Applications running at seller 108 are preferably adapted to sign messages, verify signatures on messages, and check the status of a certificate as described, for example, in copending United States patent application Serial No. 09/657,604, filed on even date herewith, entitled System and Method for Facilitating Access By Sellers to Certificate-Related

4

and Other Services, which is incorporated herein by reference, and to provide the payment services described herein.

On page 10 and continuing to page 11, starting at line 30, please replace the paragraph beginning "In a preferred embodiment" with the following amended paragraph:

In a preferred embodiment, transaction coordinator 202 is the primary interface to certificate based services provided by a participant. As described in copending United States patent application Serial No. 09/657,605, filed on even date herewith, entitled System and Method for Certificate Validation and Other Services, which is incorporated herein by reference, transaction coordinator 202 facilitates system functions like message verification, logging, billing, and authorization to all certificate based services.

On page 11, starting at line 5, please replace the paragraph beginning "Each customer certificate" with the following amended paragraph:

Each customer certificate is preferably linked to an end-user authorization system at issuing participant 102 and relying participant 104. The components of the authorization system may be determined by each participant, but typically include information on transaction types, amount limits, overrides and approvals permitted to each customer certificate. A preferred authorization approach is described in copending United States provisional patent application serial No. 60/231,313, filed on even date herewith, entitled Authorization/ Credential Service and Authorization/Credential Service Proposal, which is incorporated herein by reference.

5